MÄLARDALEN UNIVERSITY
SWEDEN

How to increase efficiency with the certification of process compliance

Barbara Gallina
School of Innovation, Design and Engineering,
Mälardalen University, Västerås, Sweden
barbara.gallina@mdh.se

2017 March 27th, Malaga University

Talk outline

- Recent Bio
- Preliminary concepts
  - Certification, process-based certification, etc.
  - Certification crisis
  - Certification framework
- Context and motivation
- Background
- THRUST/MDSafeCer
- Proof-of-concept prototype
- Conclusion and future work

Recent bio - research

- **Associate Professor** at MDH, working on Dependability
  - **Dependability modelling and analysis**
  - **ISO 26262-compliant safety case building**
  - **Systematic reuse of (Relaxed) ACID-based transactional artifacts**
  - **Systematic reuse of product-related certification artifacts**
  - **(Safety-critical) Software Development as a Service (SDaaS)**
  - **Systematic reuse of process-related certification artifact**

- Research Projects
  - EU ECSEL AMASS: Technical manager, WP/Task-leader
  - EU ARTEMIS CHESS, CONCERTO, p/nSafeCer: (co)WP/Task-leader
  - SSF SYNOPSIS, Gen&ReuseSafetyCases
  - …

Recent bio - education

- Education
  - DVA321-Safety-critical systems engineering
  - DVA433-Functional safety, PROMPT initiative
  - New course on certification (to be developed)
  - Contribution to the discussion related to the **Manifesto on Software Process Education, Training and Professionalism**
    - **Constructive Alignment extension for safety critical systems**

Preliminary concepts

- Certification
  - from Latin, certify-->make certain
  - in common use: attestation by someone trustworthy that a certain statement is true to the best of his/her knowledge

- Why Safety Certification?

"Safety certification **assures society** at large that deployment of a given system does not pose an unacceptable risk of harm. There are several ways of organizing and conducting certification, but all are conceptually based on scrutiny of an argument that certain claims about safety are justified by evidence about the system. "

Taken from J. Rushby, Substantially revised version; original appears in Proceedings of the Ninth ACM International Conference On Embedded Software (EMSOFT), pp. 211–218, Taipei, Taiwan, October 2011.

Preliminary concepts

- What can be certified in the context of safety-critical systems?
  - Processes
  - Products
  - Tools used during the development of products
    - Tool qualification processes
  - …

Why process-based certification?

- We have no real consensus on absolutely essential metrics for products.

- It is widely accepted that testing software products completely is not possible. One of the major differences between software products and more traditional, physical products, is that the principle of continuity does not apply to software products. Since software engineers felt that even a huge number of test cases could not guarantee the quality of the product, **we turned to supportive evidence**, hoping that layers of evidence will add up to more tangible proof of quality/dependability.

Taken from: A. Wassyng, T. Maibaum, and M. Lawford.
On Software Certification: We Need Product-Focused Approaches.
LNCS Vol. 6028, Springer, 2010, 250-274.

Process and process-based certification

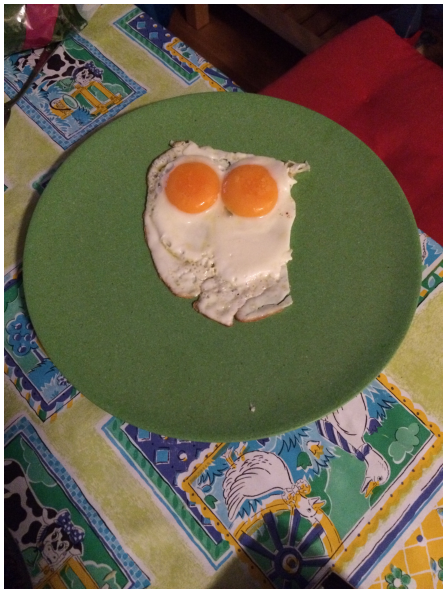
- Processes are not useful
- Documentation is not useful

Self-fulfilling prophecy[1]

[Parnas et al 1986] A RATIONAL DESIGN PROCESS: HOW AND WHY TO FAKE IT

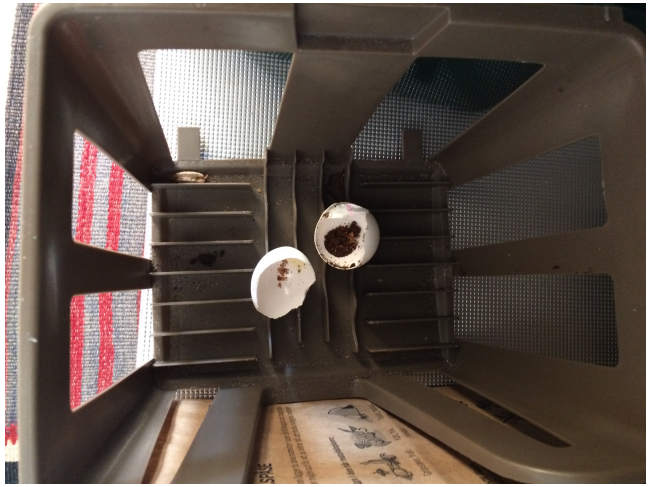
[1]A prediction that directly or indirectly causes itself to become true, by the very terms of the prophecy itself, due to positive feedback between belief and behavior

On the statement: processes are not useful



For process-inspiration, consider: https://en.wikibooks.org/wiki/Cookbook:Fried_Eggs

On the statement: processes are not useful



Time wasted! Moreover, in the meantime, I might burn the eggs,
I might eat cancerogenic substances

Process-based certification

- Which is the danger?
  - "box ticking" mentality (checklist of deliverables)

- We need product assurance instead of compliance with standards. Compliance with standards is a necessary but not a sufficient condition!
- Why is not sufficient?
  - efficacy of development approaches (UNKNOWN)
  - benefits of certification schemes (UNKNOWN)

Process-based certification

"Those seeking to reduce costs argue that some of the DO- 178B objectives or activities are unnecessary and could be eliminated. The danger is that, if we don't know why DO-178B works, we could stop doing something that really matters, which could lead to an accident." Taken from D. Daniels **"The Efficacy of DO-178B "**

"never-enough-studied process-product relationship**"**
Taken from M. Fusani & G. Lami **"On the efficacy of safety-related software standards**"

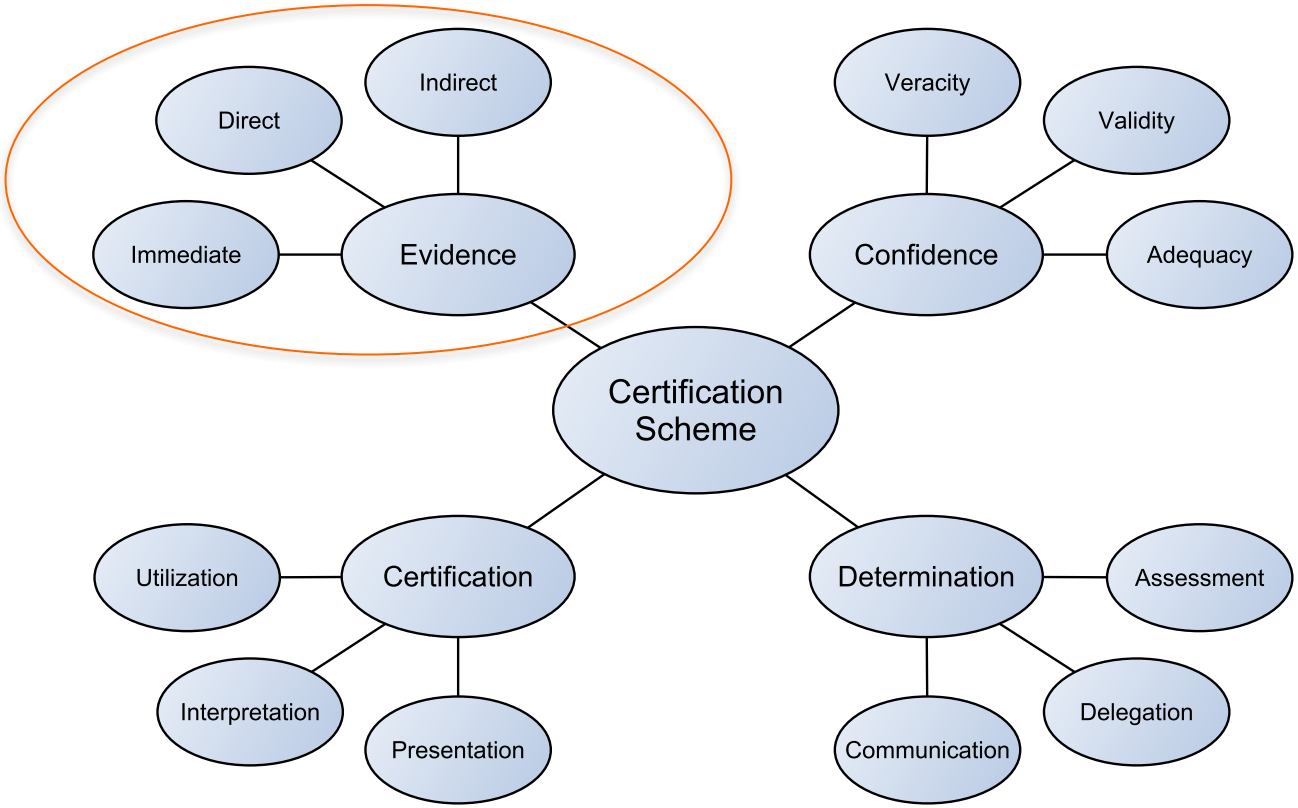
Planning the Unplanned Experiment:
Assessing the Efficacy of Standards for Safety Critical Software, EDCC workshop, 2014

Certification crisis!!!

Why?

(Increasingly, many researchers and practitioners are questioning themselves about the value of the current certification processes)

Certification framework



"..designed to allow for new measurements and analyses to be incorporated as they become available, **but also to make use of more qualitative evidence like process adherence and personnel qualifications**, etc., for the time being. "
Taken from: M. Bender, T. Maibaum, M. Lawford and A. Wassyng, "Positioning Verification in the Context of Software/System Certification", In *Proc. of the 11th International Workshop on Automated Verification of Critical Systems (AVoCS 2011), Electronic Communications of the EASST (European Association of Software Science and Technology)*, Volume 46, 2013.

Let's look at reality…

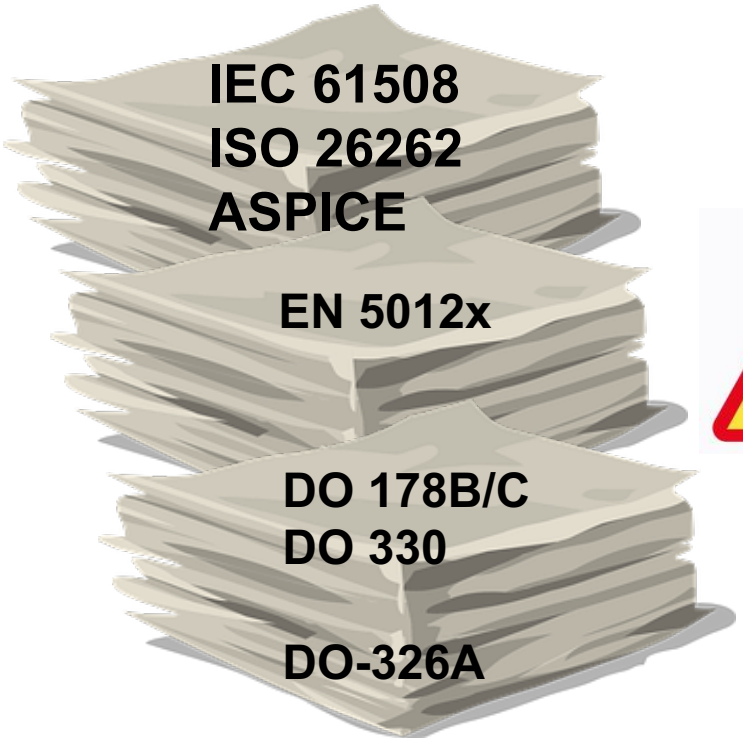
Context

Objective-based	Prescriptive, triple V model + tailoring rules	Prescriptive, V model
• DO-178B	ISO 26262-2011	BS EN 50128:2001
• DO-178C	ISO 26262-2018	BS EN 50128:2011
• …		

The original **DO-178 had sixty-seven pages**. Today's engineers working on a modern Integrated Modular Avionic (IMA) platform have to be familiar with (and in many cases comply to) over a thousand pages of official RTCA publications supported by hundreds of pages of regulatory guidance. The DO-178C family of documents alone weighs in at over **six hundred pages**.

Taken from "**Assuring Avionics – Updating the Approach for the 21st Century** " by T. Ferrell and U. Ferrell, SASSUR, 2014

Motivation



Proliferation of standards
→thousands of pages!
→increasing complexity
→intellectual unmanageability
→(re)certification is inefficient
(time consuming and expensive!)

How the proliferation of standards could be faced?

- **How complexity could be mastered?**
- **How can we speed up (re)certification?**
- **How can we enable intra/cross domain reuse?**
- **How can we enable process-related systematic reuse?**
- What varies from one criticality level to another?
- What varies from one version to another?
- What remains unchanged?
- What can be reused?
- What can be generated?

Talk outline

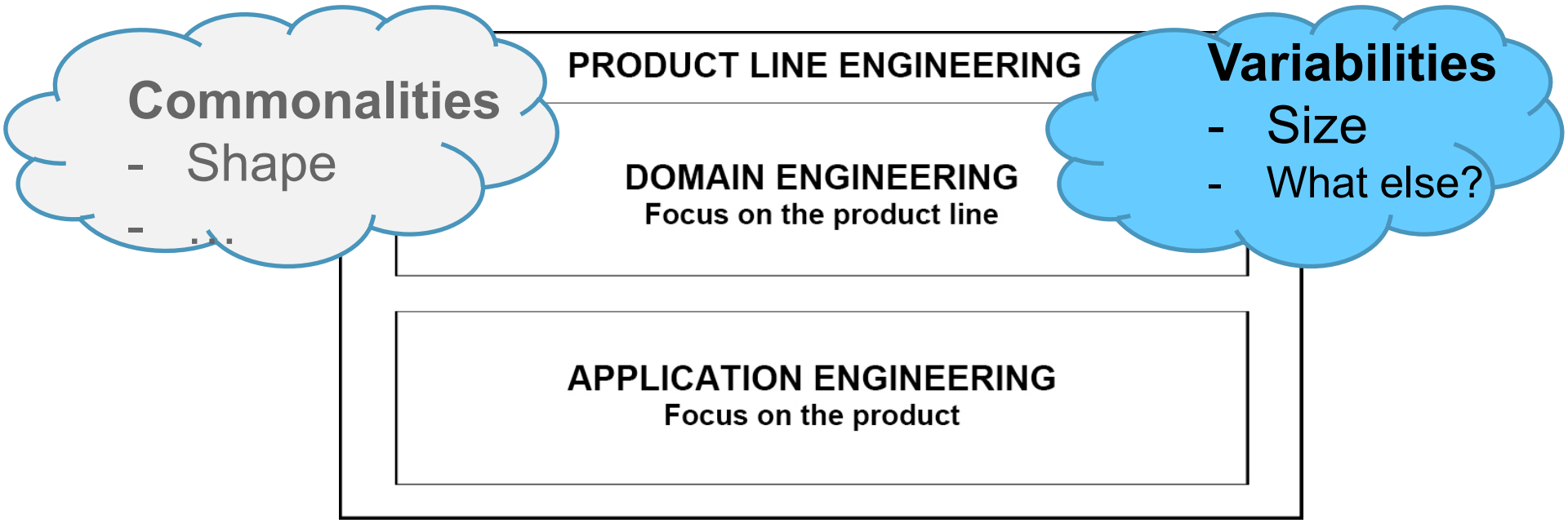
- Preliminary concepts
- Context and motivation
- Background
  - Product lines engineering
  - Safety-oriented process line engineering (SoPLE)
  - Safety-oriented process line modeling
  - Process compliance
  - Process compliance documentation
  - Model-driven Engineering/Certification
- THRUST/MDSafeCer
- Proof-of-concept prototype
- Conclusion and future work

Product lines engineering

- Concurrent engineering of a set of products
  - Why? To reuse systematically
    - To reduce time and cost, while increasing quality

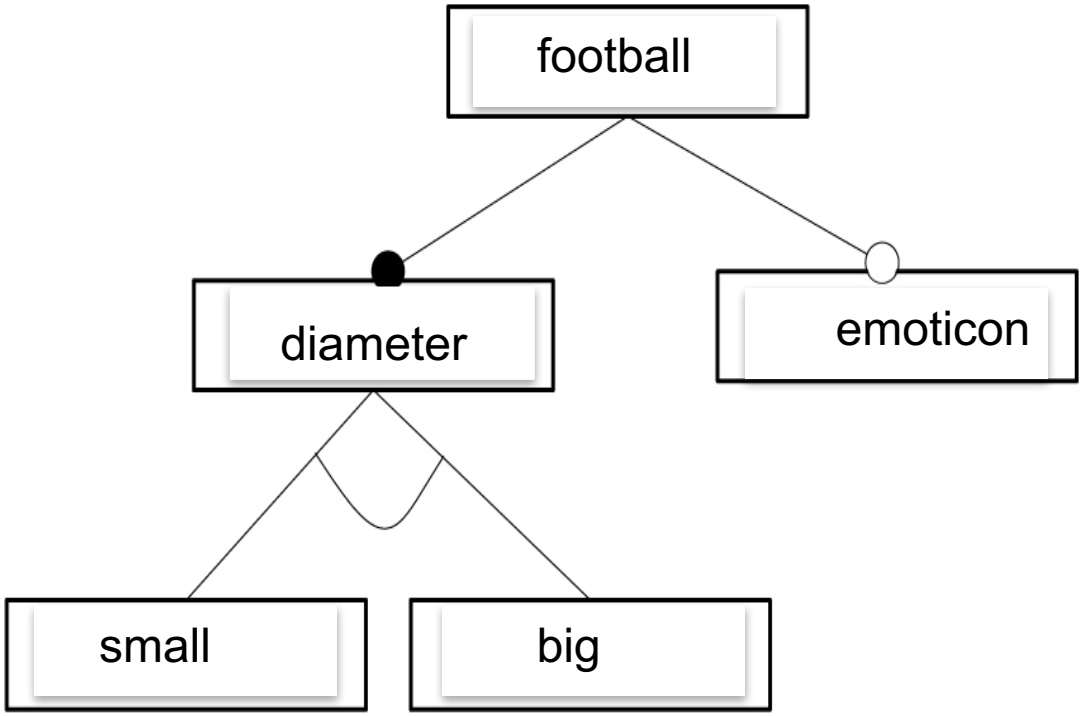
Product lines engineering

- 2-phase method



Product lines engineering

(modelling support)



P4={big, emoticon}

Safety-oriented process line engineering-SoPLE

- Concurrent engineering of a set o safety-oriented processes
  - Why? To reuse systematically!

Gallina et al 2012 (SEW Workshop)

Gallina et al 2014 (QUORS Workshop)

Gallina et al 2014 (DEVVARTS Workshop)

- Which consists of:
  - Scoping
  - Domain engineering (full and partial commonalities, variabilities)
  - Process engineering

Safety-oriented process lines modeling

- S-TunExSPEM (SPEM2.0 extension)

Task	Role	Tool	Work product	Guidance	Phase
					

Gallina et al 2014
(SERA Conference)

- vSPEM (SPEM2.0 extension)

Concept	Variation point	Variant
Task		

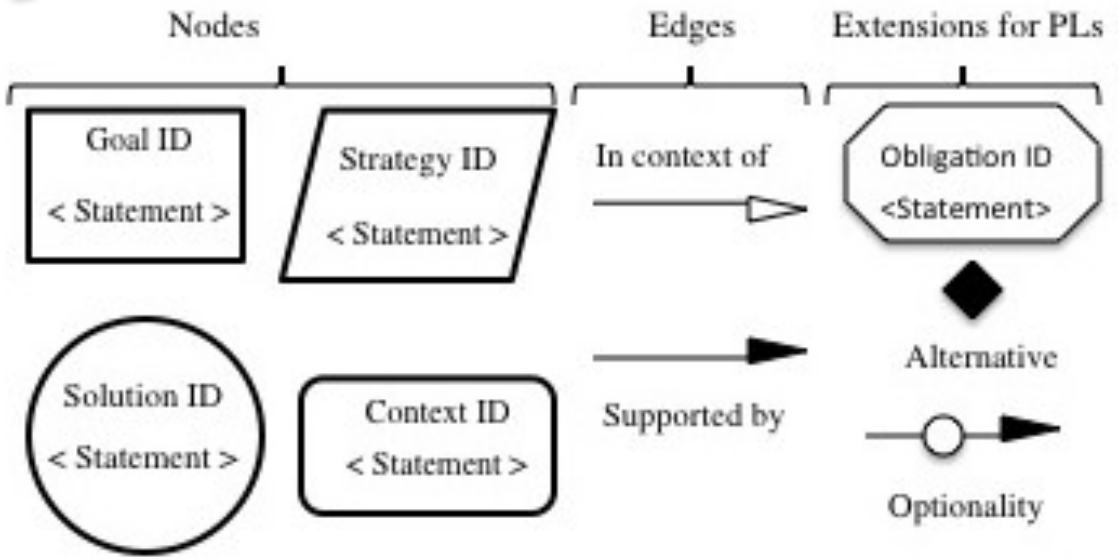
Process compliance

- To be compliant, a company has two alternatives:
  - strict and almost literal implementation of the process
    - identification and assignment of roles;
    - execution of all the activities according a specific order (if any) and/or grouping (if any);
    - consumption/provision of all the required work products;
    - application of specific guidance (if any);
    - usage of specific tools (if any).
  - **execution of a tailored process**

Process compliance documentation

- Textual languages (plain natural language)
- Graphical notations
  - CAE
  - GSN

SACM (Structured Assurance Case Metamodel) 2.0



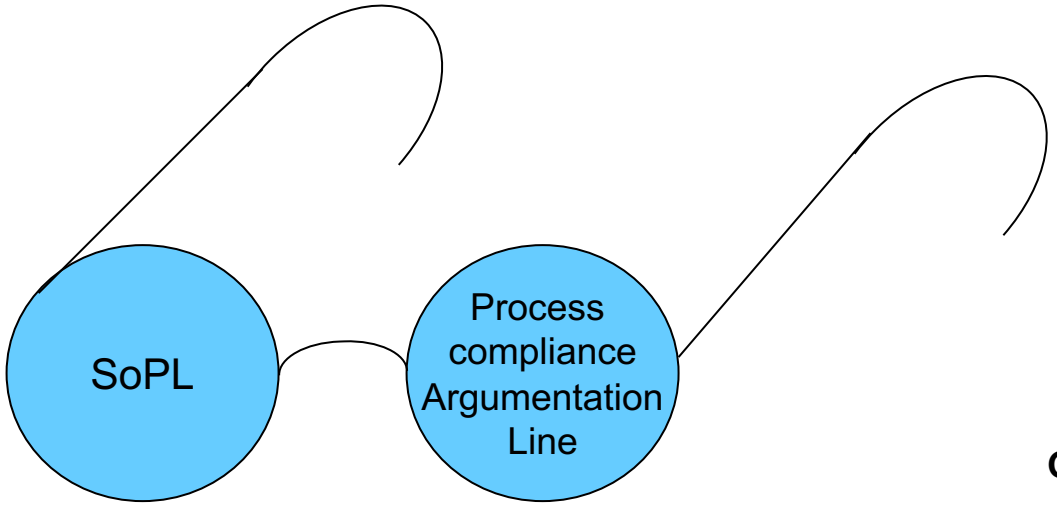
Model-driven Engineering

- MDE: Model-centric software engineering method
  - Model transformations from **source to target space**
    - Vertical transformations aimed at generating code
    - Horizontal transformation aimed at analyzing properties

Talk outline

- Background
- THRUST/MDSafeCer
  - Overview
  - Process
  - Applications
  - Take home message
- Proof-of-concept prototype
- Conclusion and future work

THRUST



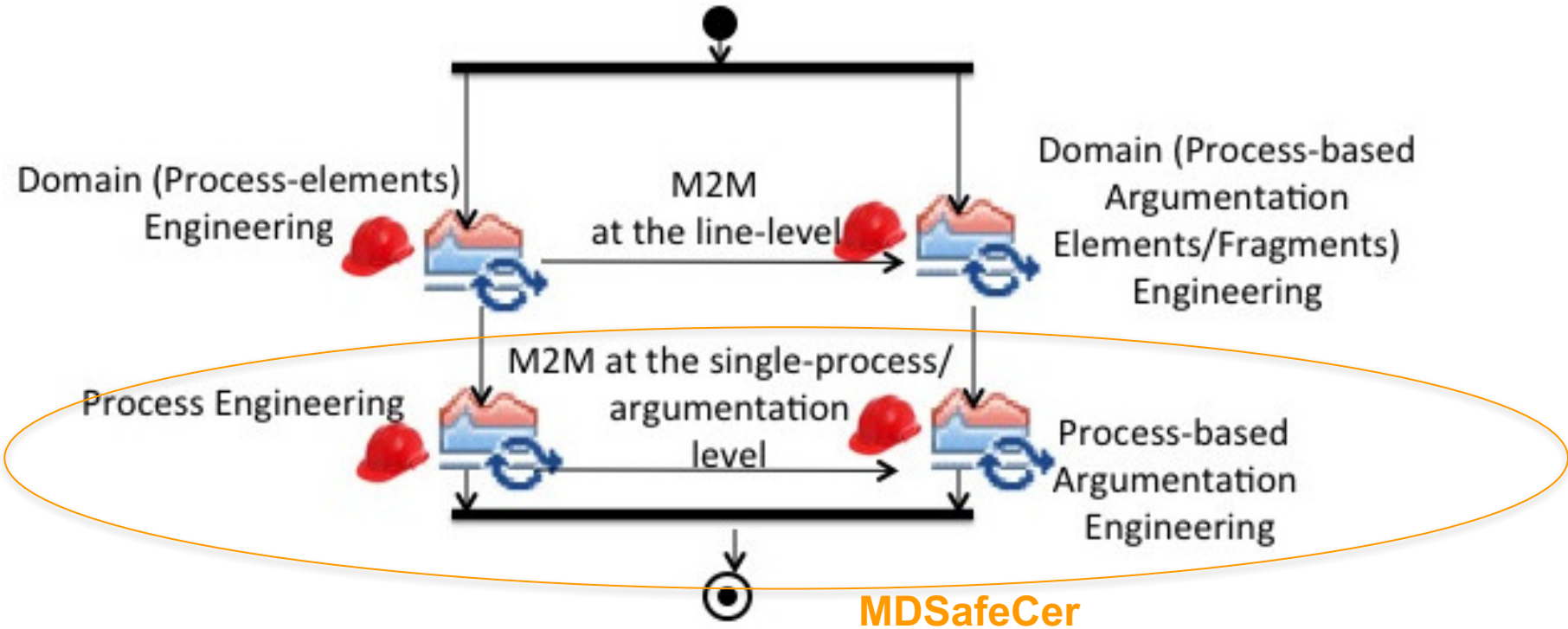
Gallina et al 2014 (DASC Conference)

+ model-driven principles…

THRUST

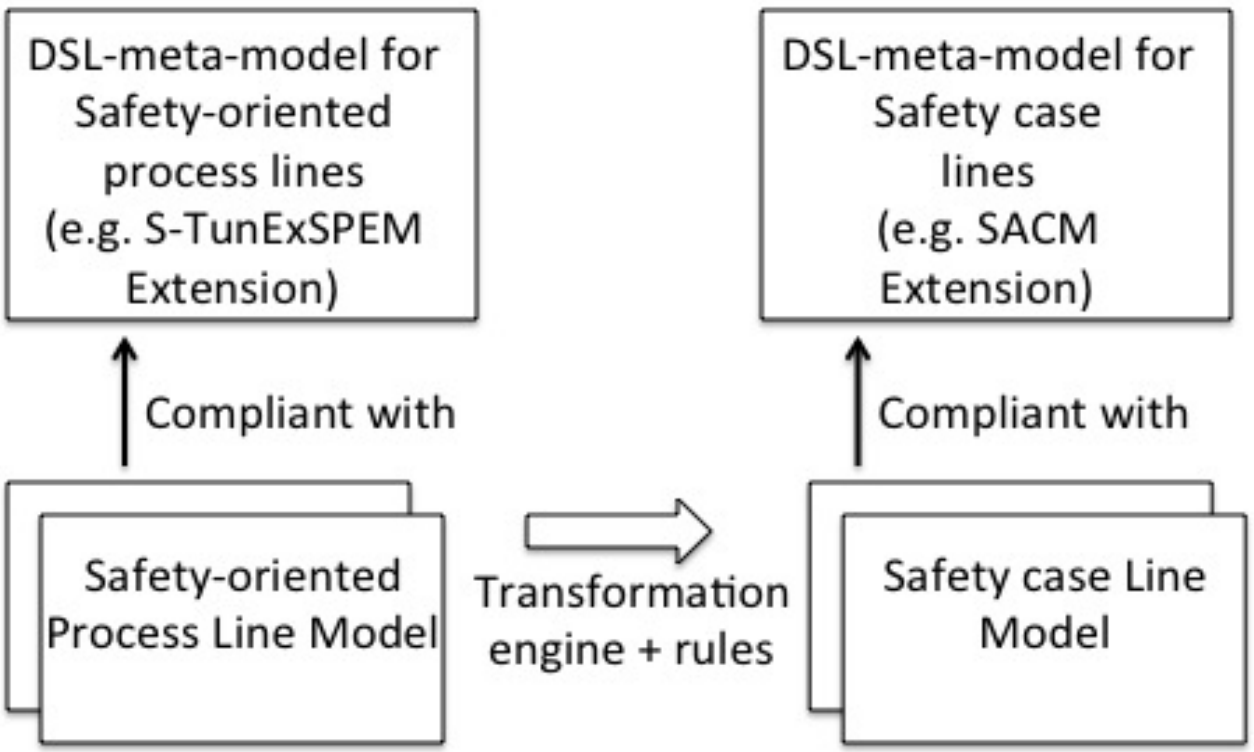
- Method for speeding up the creation of process-based artefacts via:
  - Systematic reuse
    - safety-oriented process lines
    - safety argumentation lines
  - Semi-automatic generation
    - model driven certification

THRUST

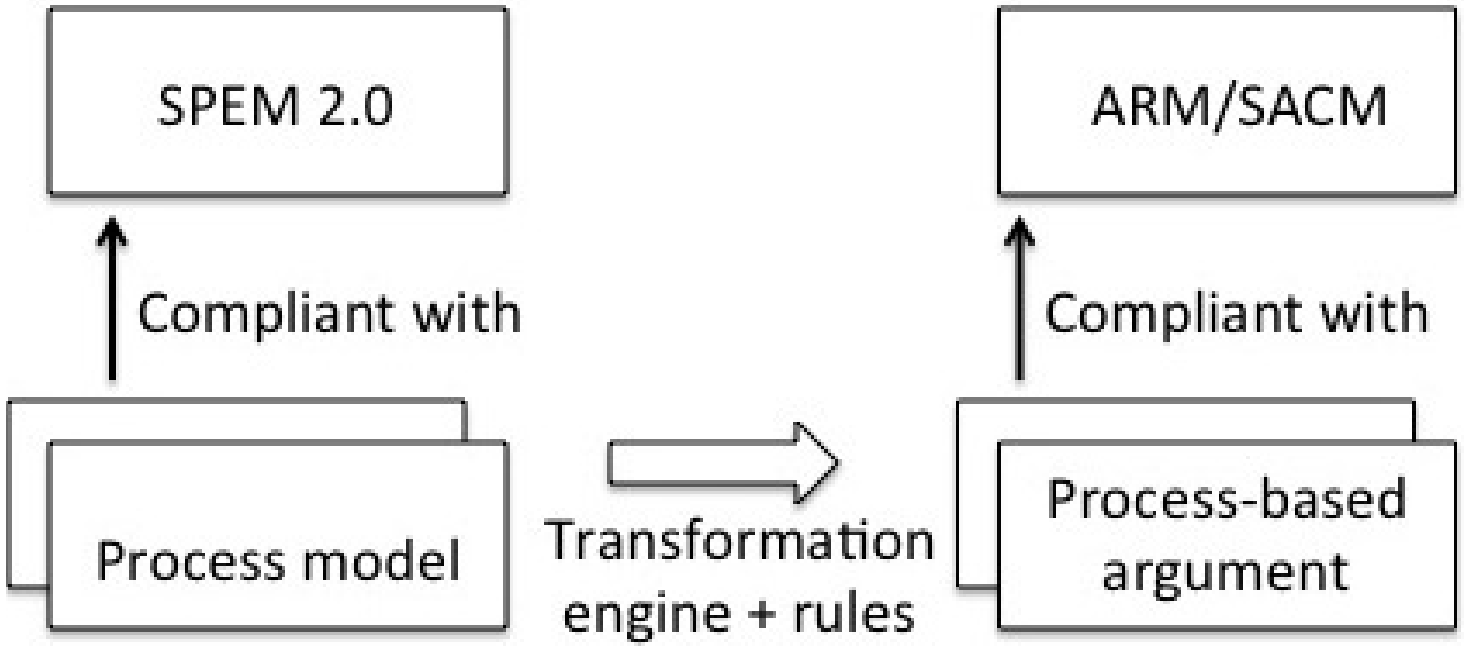


MDSafeCer
(Gallina 2014, ASSURE Workshop)

THRUST


DSL-meta-model for Safety-oriented process lines (e.g. S-TunExSPEM Extension)
DSL-meta-model for Safety case lines (e.g. SACM Extension)
Compliant with
Compliant with
Safety-oriented Process Line Model
Transformation engine + rules
Safety case Line Model

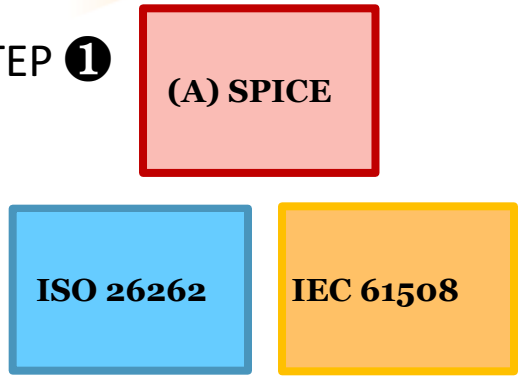
MDSafeCer



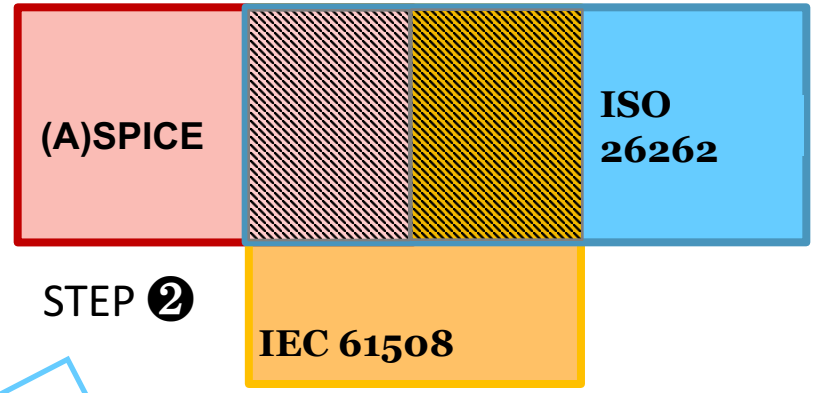
Gallina
(ASSURE Workshop)

Automotive Safety oriented Process Line Engineering
Focus on development processes

STEP ❶

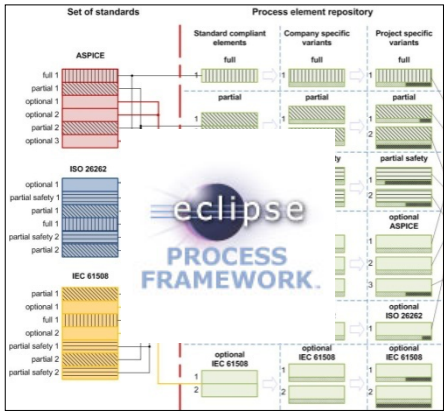


STEP ❷



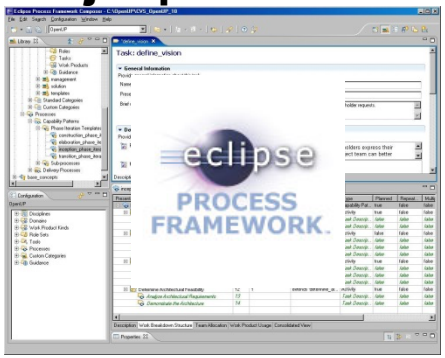
STEP ❸

STEP ❹ - ❻



STEP ❼

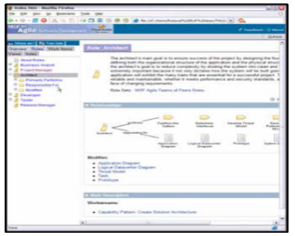
Proj. Spec. Process



STEP ❽

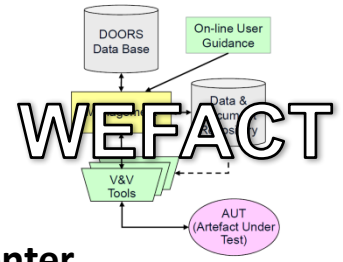
EXPORT HTML

Guideline



STEP ❾

EXPORT XML



Work in cooperation with Virtual Vehicle Research Center

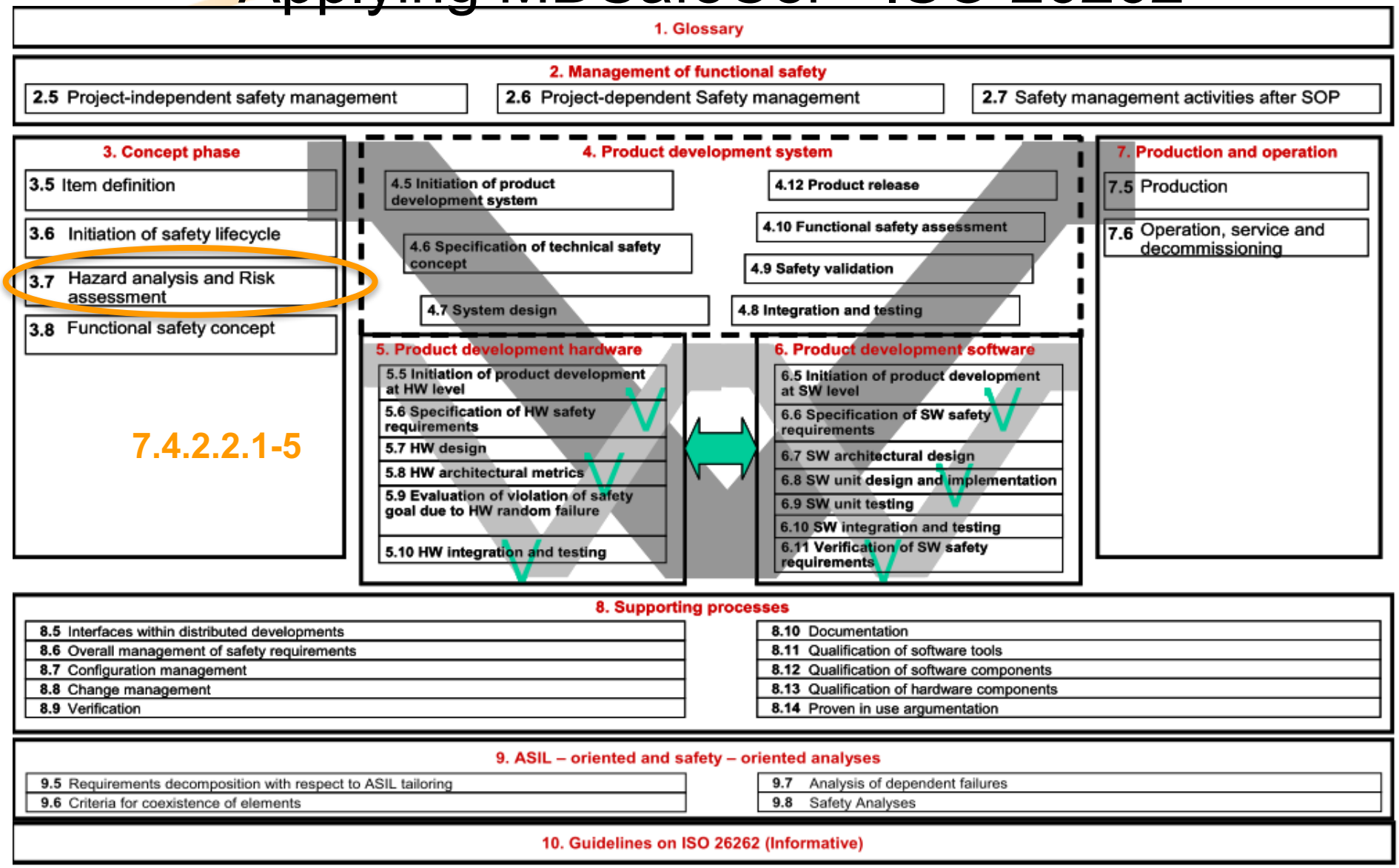
Applying MDSafeCer - ISO 26262

- Concerning process compliance, in ISO 26262 we can read:
  - The organization shall institute, execute and maintain organization-specific rules and processes to comply with the requirements of ISO 26262 (Part 2, 5.4.2.2).
  - Organization-specific rules and processes for functional safety is a specific work-product that must be provided (Part 2, 5.5.1).
  - A functional **safety audit** shall be carried out for items, where the highest ASIL of the item's safety goals is ASIL (B), C, or D, in accordance with 6.4.7, 6.4.3.5 i) and 6.4.8.2. (Part 2, 6.4.8.1), where a functional safety audit is a work-product aimed at evaluating the process implementation.
  - The organization may tailor the safety lifecycle (Part 2, 5.4.5.1) and tailoring rules are then detailed.

Thus, for certification purposes, it is crucial to provide work-products aimed at showing that either process activities have been performed according to the ISO 26262 safety life-cycle or they have been tailored appropriately according to the tailoring rules provided within ISO 26262.

MÄLARDALEN UNIVERSITY
SWEDEN

Applying MDSafeCer - ISO 26262



Applying MDSafeCer - ISO 26262

1. Create the top-level goal ID:G1 and statement: "The task *ta* has been carried out". Create the context to be associated to G1. Context ID:C1 and statement: "Standard {x}", where x is a variable. Create an inContextOf link to relate G1 and C1.

Develop the goal G1 further by creating four strategies and for each strategy a set of sub-goals.

(a) S1: "Argument over roles R".

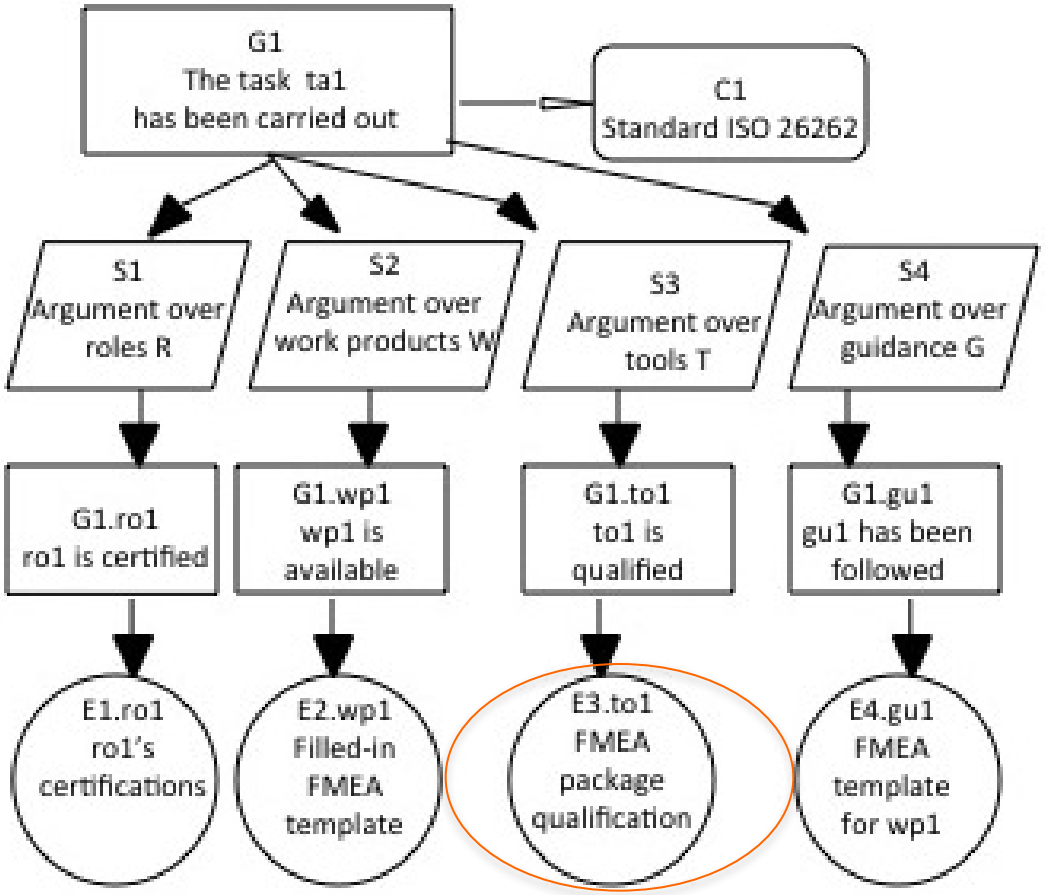
(b) S2: "Argument over work products W".

(c) S3: "Argument over tools T".

(d) S4: "Argument over guidance G".

Applying MDSafeCer - ISO 26262

(towards a process-based argumentation pattern)



Contracts?
Modules?
Justifications?
Assumptions?
Undeveloped goals?

Proof-of-concept prototype

- Implementation within AIT-WEFACT-tool

  Work in cooperation with:

  Austrian Institute of Technology (AIT)

  Virtual Vehicle Research Center (ViF)

http://www.ait.ac.at/research-services/research-services-digital-safety-security/verification-and-validation/methods-and-tools/wefact-workflow-engine-for-analysis-certification-and-test/?L=1

- Implementation within the SDaaS-prototype architecture

Take home message

- SoPLE+MDSafeCer may contribute in increasing efficiency

- More efficiency in process certification→
  More time for product-based evidence provision!!
  →e.g., verification results

- SoPLE may contribute in:
  - Re-establishing a balance between the "odd couple" (discipline and creativity)
  - Enabling a transition "from rigid compliance to smart convergence"
  - Enabling a transition from non rationalized standards to **rationalized standards**

R. Conradi & A. Fuggetta. Improving Software Process Improvement. IEEE Software, 2002.
A. Fuggetta & E. Di Nitto. Software process. In *Proc. of Future of Software Engineering* (FOSE), 2014.
J. C. Knight, J. C. Rowanhill. The Indispensable Role of Rationale in Safety Standards. SAFECOMP, 2016.

Conclusion

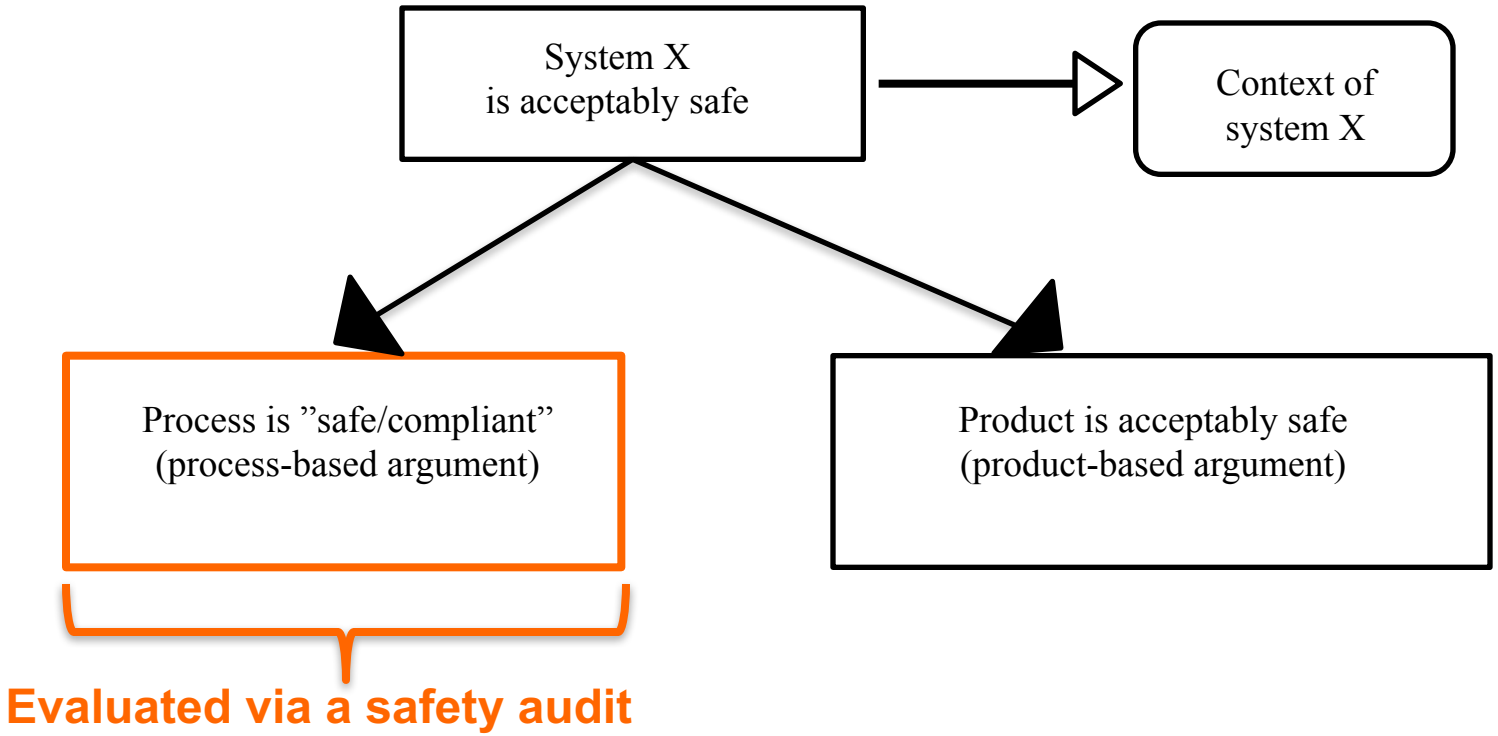
- THRUST/MDSafeCer:
  - Novel model-driven approaches for time and cost reduction
    - Mapping of (ideally reusable) process structures (patterns) onto (ideally reusable) argumentation structures (patterns)
- Manual application on various small-sized sub-processes
  - Automotive
  - Rail
  - Avionics
  - Space
- Prototype tool support – proof of concepts
  - Initial validation

Future work

- Provision of a fully defined pattern for process compliance
- Contribution to provision of adequate metamodels
- Experimental validation on more complex case-studies

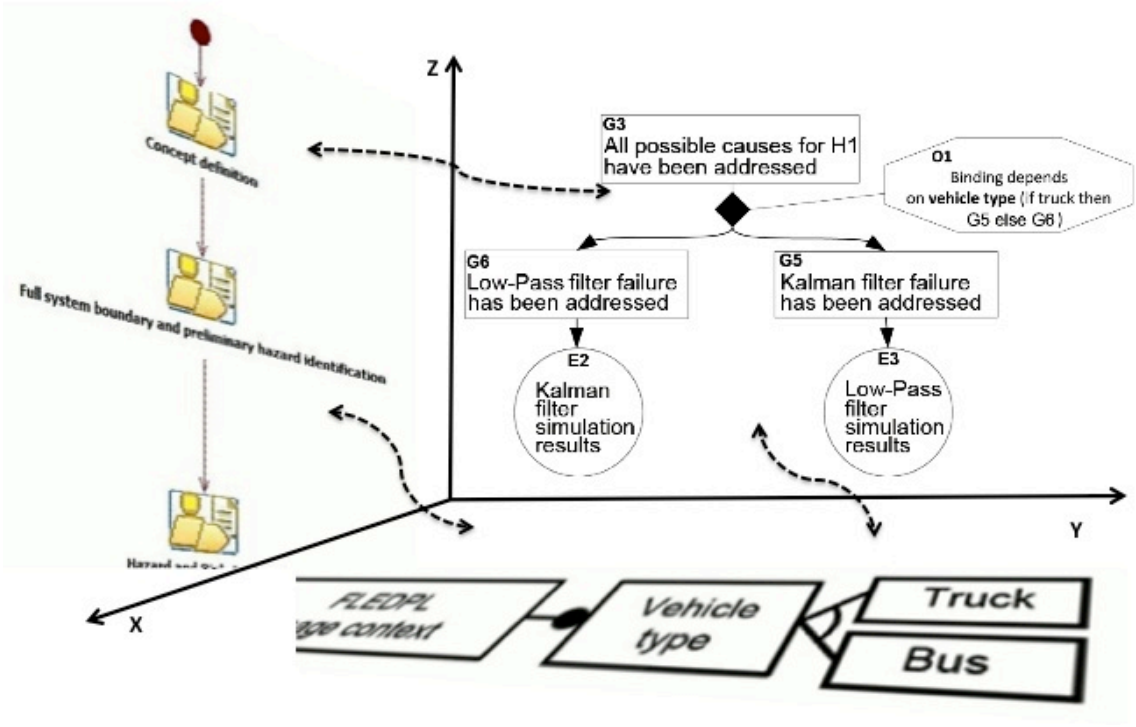
- Towards Anti-Sisyphus: combination of
  - safety-oriented process lines,
  - safety-critical product lines,
  - safety case lines

Safety case
(core arguments)



Fragment of a goal structure, safety argument given in GSN (Goal Structuring Notation)

Anti-Sisyphus



Gallina 2015
(PLEASE Workshop)

Then, proposed at the brokerage event at MDH,
http://www.mrtc.mdh.se/es_brokerage/presentations/11_ES_brokerage_Anti-Sisyphus_Barbara_Gallina.pdf
Then, integrated within AMASS (http://www.amass-ecsel.eu), see AMASS newsletter 1.

Thank you for your attention!

Discussion time…

Publications

International Peer-reviewed Journals

1. **B. Gallina**, E. Gómez-Martínez, C. Benac Earle. Promoting MBA in the Rail Sector by Deriving Process-related Evidence via MDSafeCer. Computer Standards & Interfaces -SPICE-2016 Special Issue (CSI SPICE-2016), http://dx.doi.org/10.1016/j.csi.2016.11.007;
2. **B. Gallina**, L. Provenzano. Deriving Reusable Process-based Arguments from Process Models in the Context of Railway Safety Standards. Ada User Journal, vol 36, n. 4, 2015.

Publications

International Peer-reviewed Conferences

1. **B. Gallina**, A. Andrews. Deriving Verification-related Means of Compliance for a Model-based Testing Process. IEEE 35th Digital Avionics Systems Conference (DASC), Sacramento, CA, US, September 25-29, 2016.
2. S. Alajarami, A. Romanovsky, and **B. Gallina**. Software Development in the Post-PC Era: Towards Software Development as a Service. Proceedings of the 17th International Conference on Product-Focused Software Process Improvement (PROFES), Springer, LNCS, Bolzano, Italy, November 24-26, 2016.
3. S. Alajrami, **B. Gallina**, I. Sljivo, A. Romanovsky, P. Isberg. Towards Cloud-Based Enactment of Safety-Related Processes. Proceedings of the 35th International Conference on Computer Safety, Reliability and Security (SafeComp), Trondheim, Norway, September 20-23, 2016.
4. **B. Gallina**, E. Gomez-Martınez, and C. Benac Earle. Deriving Safety Case Fragments for Assessing MBASafe's Compliance with EN 50128. 16th International SPICE Conference on Process Improvement and Capability dEtermination (SPICE), Dublin, Ireland, Vol. 609, Communications in Computer and Information Science series, pp. 3-16, ISBN 978-3-319-38979-0, Springer, 2016.

Publications

International Peer-reviewed Conferences

5. S. Alajrami, **B. Gallina** and A. Romanovsky. EXE-SPEM: Towards Cloud-Based Executable Software Process Models. 4th International Conference on Model-Driven Engineering and Software Development (MODELSWARD), SCITEPRESS, Rome, Italy, 19-21 February, 2016.
6. **B. Gallina**, Z. Szatmari. Ontology-based Identification of Commonalities and Variabilities among Safety Processes. Proceedings of the 16th International Conference on Product-Focused Software Process Improvement (PROFES), Springer, LNCS 9459, pp. 182-189, ISBN 978-3-319-26843-9, Bolzano, Italy, December 2-4, 2015.
7. **B. Gallina**, L. Fabre. Benefits of Security-informed Safety-oriented Process Line Engineering. IEEE 34th Digital Avionics Systems Conference (DASC-34), Prague, Czech Republic, September 13-17, ISBN 978-1-4799-8939-3, 2015.
8. **B. Gallina**, L. Provenzano. Deriving Reusable Process-based Arguments from Process Models in the Context of Railway Safety Standards. 20th International Conference on Reliable Software Technologies-Industrial Presentation- (Ada-Europe-2015), Madrid, Spain, June, 2015.

Publications

International Peer-reviewed Conferences

- **B. Gallina**, Lundqvist and K. Forsberg. THRUST: A Method for Speeding Up the Creation of Process-related Deliverables. IEEE 33rd Digital Avionics Systems Conference (DASC-33), doi:10.1109/DASC.2014.6979489, Colorado Springs, CO, USA, October 5-9, 2014.
- **B. Gallina**, K. R. Pitchai and K. Lundqvist. S-TunExSPEM: Towards an Extension of SPEM 2.0 to Model and Exchange Tuneable Safety-oriented Processes. 11th International Conference on Software Engineering Research, Management and Applications (SERA), SCI 496, Springer, ISBN 978-3-319-00947-6, Prague, Czech Republic, August 7-9, 2013.

International Peer-reviewed Workshops

- A. Ruiz Lopez, **B. Gallina**, J. Luis de la Vara, S. Mazzini, H. Espinoza Ortiz. AMASS: Architecture-driven, Multi-concern, Seamless, Reuse-Oriented Assurance and Certification of CPSs. 5th International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems (SASSUR), Trondheim, Norway, September, 2016.
- **B. Gallina**. Towards Enabling Reuse in the Context of Safety-critical Product Lines. 5th International Workshop on Product LinE Approaches in Software Engineering (PLEASE), joint event of ICSE, Florence, Italy, May 19th, 2015.

Publications

International Peer-reviewed Workshops

- **B. Gallina**. A Model-driven Safety Certification Method for Process Compliance. 2nd IEEE International Workshop on Assurance Cases for Software-intensive Systems (ASSURE), joint event of ISSRE, Naples, Italy, doi: 10.1109/ISSREW.2014.30, pp. 204-209, November 3-6, 2014.
- **B. Gallina**, S. Kashiyarandi, K. Zugsbrati and A. Geven. Enabling Cross-domain Reuse of Tool Qualification Certification Artefacts. Proceedings of the 1st International Workshop on DEvelopment, Verification and VAlidation of cRiTical Systems (DEVVARTS), joint workshop at SafeComp conference, Springer, LNCS 8696, ISBN: 978-3-319-10556-7, pp. 255-266, Florence (Italy), 8 September, 2014.
- **B. Gallina**, S. Kashiyarandi, H. Martin and R. Bramberger. Modeling a Safety- and Automotive-oriented Process Line to Enable Reuse and Flexible Process Derivation. Proceedings of the 8th IEEE International Workshop on Quality-Oriented Reuse of Software (QUORS), joint workshop at COMPSAC conference, IEEE Computer Society, doi: 10.1109/COMPSACW.2014.84, pp. 504-509,Västerås (Sweden), 2014.
- **B. Gallina**, I. Sljivo, and O. Jaradat. Towards a Safety-oriented Process Line for Enabling Reuse in Safety Critical Systems Development and Certification. Post-proceedings of the 35th IEEE Software Engineering Workshop (SEW-35), IEEE Computer Society, ISBN 978-1-4673-5574-2, Heraclion, Crete (Greece), 2012.